

Notice of Allowability

Application No.

09/846,175

Examiner

Beemnet W. Dada

Applicant(s)

BREZAK ET AL.

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 08/08/07.
2. ☒ The allowed claim(s) is/are 1,2,5-9,11,12,15-19,21,22 and 25.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Beatrice L. Loempel-Thomas on 09/25/07.

The application has been amended as follows:

In the claims:

1. **(Currently Amended)** A method for use in a computer capable of supporting multiple authentication mechanisms, the method comprising:
generating at least one [indicator] access token that identifies a user, and is associated with and identifies at least one authentication mechanism that has been used to authenticate the user, wherein generating the [indicator] access token further includes identifying within the [indicator] access token at least one characteristic associated with the authentication mechanism, wherein the at least one characteristic associated with the authentication mechanism includes a measure of strength of the authentication mechanism, wherein the measure of strength of the authentication mechanism depends on the length of key employed in an encryption process; and
controlling the user's access to at least one resource based on the [indicator] access token.

2. (Currently Amended) The method as recited in Claim 1, wherein generating the [indicator] access token further includes receiving inputs, providing the inputs to the authentication mechanism, and causing the authentication mechanism to generate at least one security identifier (SID) that identifies the authentication mechanism.

3. (Canceled).

4. (Canceled).

5. (Previously Presented) The method as recited in Claim 1, wherein the measure of strength of the authentication mechanism identifies a length of an encryption key employed by the authentication mechanism.

6. (Currently Amended) The method as recited in Claim 1, wherein controlling access to the resource based on the [indicator] access token further includes comparing the [indicator] access token to at least one access control list having at least one access control entry therein.

7. (Original) The method as recited in Claim 6, wherein if the access control entry operatively specifies that the at least one authentication mechanism is permitted to access the resource, then access to the at least one resource is allowed to proceed.

8. (Original) The method as recited in Claim 6, wherein if the access control entry operatively specifies that the at least one authentication mechanism is not permitted to access the resource, then access to the at least one resource is not allowed to proceed.

9. (Original) The method as recited in Claim 6, wherein if the access control entry does not operatively specify that the at least one authentication mechanism is permitted to access the resource, then access to the at least one resource is not allowed to proceed.

10. (Canceled)

11. (Currently Amended) A computer-readable medium for use in a device capable of supporting multiple authentication mechanisms, the computer-readable medium having computer-executable instructions for performing acts comprising:

producing at least one [indicator] access token that identifies a user, and uniquely identifies at least one authentication mechanism supported by the device that has been used to authenticate the user, wherein producing the [indicator] access token further includes identifying within the [indicator] access token at least one characteristic of the authentication mechanism, wherein the at least one characteristic of the authentication mechanism includes a strength characteristic of the authentication mechanism, wherein the strength characteristic of the authentication mechanism depends on the length of key employed in an encryption process; and

causing the device to selectively control the user's access to at least one resource operatively coupled to the device based at least in part on the [indicator] access token.

12. (Original) The computer-readable medium as recited in Claim 11, wherein producing the [indicator] access token further includes receiving inputs, providing the inputs to the authentication mechanism, and causing the authentication mechanism to generate at least one security identifier (SID) that identifies the authentication mechanism, in response thereto.

13. (Canceled).

14. (Canceled).

15. (Previously Presented) The computer-readable medium as recited in Claim 12, wherein the strength characteristic identifies a length of an encryption key employed by the authentication mechanism.

16. (Currently Amended) The computer-readable medium as recited in Claim 11, wherein causing the device to selectively control access to the at least one resource based on the [indicator] access token further includes causing the device to compare the [indicator] access token to control data.

17. (Original) The computer-readable medium as recited in Claim 16, wherein if the control data specifies that the authentication mechanism is permitted to access the resource, to which subsequent access to the resource is allowed.

Art Unit: 2135

18. (Original) The computer-readable medium as recited in Claim 16, wherein if the control data operatively specifies that the authentication mechanism is not permitted to access the resource, to which subsequent access to the resource is prohibited.

19. (Original) The computer-readable medium as recited in Claim 16, wherein if the control data does not operatively specify that the authentication mechanism is permitted to access the resource, to which subsequent access to the resource is prohibited.

20. (Canceled)

21. (Currently Amended) An apparatus comprising:

at least one authentication mechanism facilitating generation of at least one [indicator] access token that identifies a user, and identifies the authentication mechanism that has been used to authenticate the user, wherein the [indicator] access token further includes at least one identifying characteristic associated with the authentication mechanism, wherein the at least one identifying characteristic associated with the authentication mechanism indicates a measure of strength of the authentication mechanism, wherein the measure of strength of the authentication mechanism depends on the length of key employed in an encryption process;

an access control list;

at least one access controlled resource; and

logic operatively facilitating comparison of the [indicator] access token with the access control list and selectively control the user's access to the resource based on the [indicator] access token.

22. (Original) The apparatus as recited in Claim 21, wherein the authentication mechanism is further configured to receive user inputs and generate at least one security identifier (SID) that identifies the authentication mechanism based on the user inputs.

23. (Canceled).

24. (Canceled).

25. (Previously Presented) The apparatus as recited in Claim 21, wherein the measure of strength of the authentication mechanism identifies a length of an encryption key employed by the authentication mechanism.

26. (Canceled)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W. Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

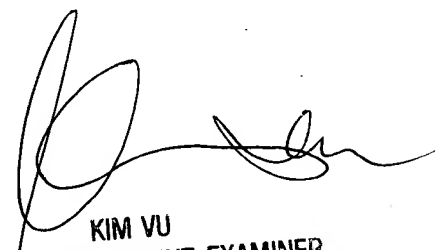
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Beemnet W Dada

September 25, 2007



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100